

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-228674

(43)Date of publication of application : 15.08.2000

(51)Int.Cl. H04L 12/56
H04L 12/46
H04L 12/28
H04L 12/66

(21)Application number : 11-027968

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 04.02.1999

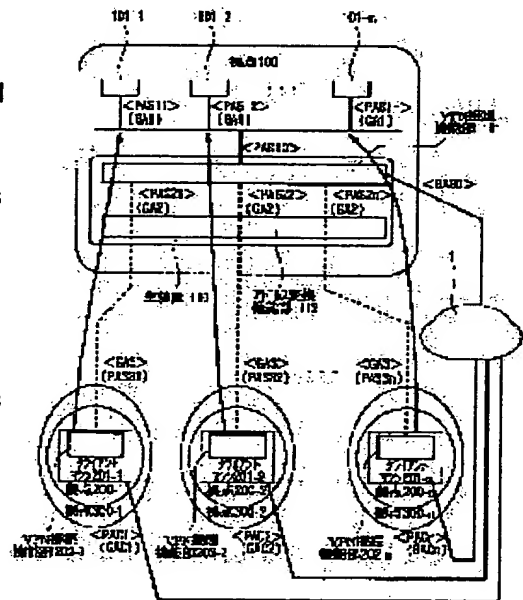
(72)Inventor : OKADA KOICHI
NAKAYAMA RYUJI

(54) ADDRESS ALLOCATING METHOD IN INTER-PLURAL POINT COMMUNICATION, COMMUNICATING METHOD AMONG PLURAL POINTS AND ITS CONNECTING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce the setting burden of 2nd point sides by allocating an address which is different from that of a destination terminal connected to a terminal in the 2nd points but common among all of the 2nd points.

SOLUTION: 2nd points 200 respectively have an address converting part such as PROXY server and fire wall for converting the private address of a client machine 201 into a global address. In a network connecting plural points, connection destinations of communication data having the same connection destination address are divided by converting the connection destination address into the address of a connection destination terminal for the communication data on a communication path between one point to which the terminal to be a connection destination candidate belongs and a connection source. Thus, it is possible for the 2nd points 200 to easily and directly communicate with a network 1 and to construct a virtual private network(VPN).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-228674
(P2000-228674A)

(43) 公開日 平成12年8月15日 (2000.8.15)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 D 5 K 0 3 0
12/46		11/00	3 1 0 C 5 K 0 3 3
12/28		11/20	B 9 A 0 0 1
12/66			

審査請求 未請求 請求項の数18 O L (全 12 頁)

(21) 出願番号 特願平11-27968

(22) 出願日 平成11年2月4日 (1999.2.4)

(71) 出願人 000004226

日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(72) 発明者 岡田 浩一

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 中山 隆二

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100069981

弁理士 吉田 精孝

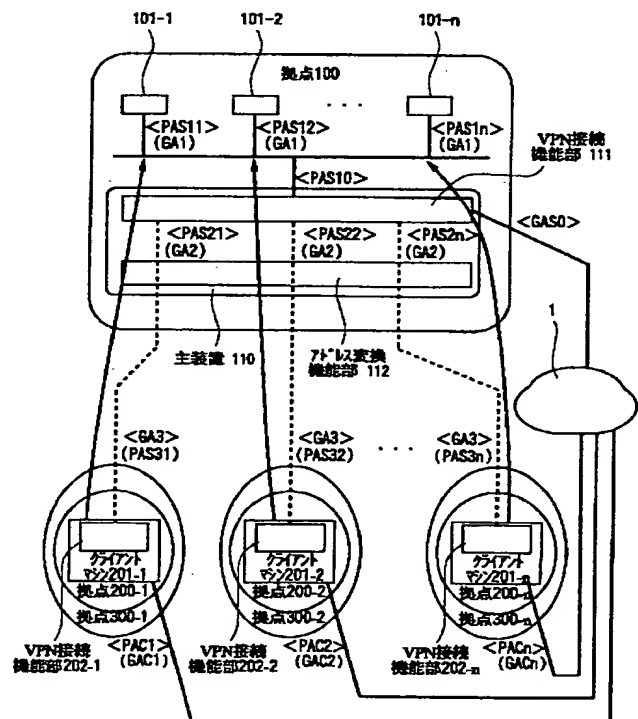
最終頁に続く

(54) 【発明の名称】 複数拠点間通信におけるアドレス割り当て方法及び複数拠点間の通信方法並びにその接続装置

(57) 【要約】

【課題】 拠点間でプライベートアドレスが重複することなく、かつグローバルアドレスを大量消費することなく、複数拠点間の通信方法及び接続装置を提供する。

【解決手段】 複数の拠点間を接続したネットワークにおいて、接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データに対して、その接続先アドレスを接続先端末のアドレスに変換することにより同一の接続先アドレスを有する通信データの接続先を振り分ける。



【 特許請求の範囲】

【請求項1】 第1の拠点と複数の第2の拠点とがそれぞれVPN(Virtual Private Network) を介して接続されたネットワークにおける複数拠点間通信において、前記第2の拠点では一の端末のみがVPN接続を行うとともに、この端末が第1の拠点における特定の端末と接続する場合には、

全ての第2の拠点におけるVPNトンネルに付加される仮想インタフェイスに対して同一のアドレスを割り当てるとともに、第2の拠点における端末の接続先となる端末に対して前記アドレスとは異なるとともに全ての第2の拠点間で共通なアドレスを割り当ててことを特徴とする複数拠点通信におけるアドレス割り当て方法。

【請求項2】 第1の拠点と第2の拠点とがそれぞれVPNを介して接続されたネットワークにおける複数拠点間通信において、

前記第2の拠点を包含する第3の拠点内において未申請のグローバルアドレスが使用されておらず、この第2の拠点では一の端末のみが第1の拠点に対してVPN接続を行う場合には、

VPN接続の際に、第2の拠点が新たに意識する第1の拠点内の端末に対して申請済みグローバルアドレスを別名アドレスとして割り当ててことを特徴とする複数拠点間通信におけるアドレス割り当て方法。

【請求項3】 第1の拠点と第2の拠点間を接続したネットワークにおける複数拠点間の通信方法において、接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データであって同一の接続先アドレスを有する通信データに対して、その接続先アドレスを接続先端末のアドレスに変換することにより通信データの接続先を振り分けることを特徴とする複数拠点間の通信方法。

【請求項4】 第1の拠点と第2の拠点間を接続したネットワークにおける複数拠点間の通信方法において、接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データであって同一の接続先アドレスを有する通信データについて、該通信データの通信経路に基づき接続先を振り分けることを特徴とする複数拠点間の通信方法。

【請求項5】 第1の拠点と第2の拠点間を接続したネットワークにおける複数拠点間の通信方法において、接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データであって同一の接続先アドレスを有する通信データに対して、その接続先アドレスを、該通信データの通信経路に対応する接続先端末のアドレスに変換することにより通信データの接続先を振り分けることを特徴とする複数拠点間の通信方法。

【請求項6】 前記第1の拠点と第2の拠点間をVPNで接続し、前記通信経路をVPNトンネルとしたことを特徴とする請求項3～5 何れか1項記載の複数拠点間の

通信方法。

【請求項7】 前記アドレス変換では、請求項1又は請求項2記載の複数拠点通信におけるアドレス割り当て方法により割り当てたアドレスに基づき、VPNトンネルを通過する通信データの送信先又は送信元アドレスを変換することを特徴とする請求項6記載の複数拠点間の通信方法

【請求項8】 前記アドレス変換の際に用いる全ての別名アドレスを第1の拠点側で予め用意することを特徴とする請求項3又は5～7 何れか1項記載の複数拠点間の通信方法。

【請求項9】 第2の拠点を複数の部分拠点に分離するとともに、各部分拠点から個別に第1の拠点に対してVPN接続を行うことを特徴とする請求項3～8 何れか1項記載の複数拠点間の通信方法。

【請求項10】 第1の拠点を經由することにより複数の第2の拠点間の通信を行うことを特徴とする請求項3～9 何れか1項記載の複数拠点間の通信方法。

【請求項11】 複数の拠点間を接続したネットワークにおける複数拠点間の接続装置であって、

接続先の候補となる端末が属する一の拠点と接続元との通信経路上の通信データに対して、その接続先アドレスを接続先端末のアドレスに変換することにより同一の接続先アドレスを有する通信データの接続先を振り分ける振り分け手段を有することを特徴とする複数拠点間の接続装置。

【請求項12】 第1の拠点と第2の拠点とがそれぞれVPNを介して接続されたネットワークにおいて第1の拠点とグローバルネットワークとを接続する接続装置であって、

VPNトンネル内を通過する通信データの送信元又は送信先アドレスをVPN接続ごとに変換するアドレス変換手段を有することを特徴とする複数拠点間の接続装置。

【請求項13】 前記第2の拠点では一の端末のみがVPN接続を行うとともに、この端末が第1の拠点における特定の端末と接続する場合において、

全ての第2の拠点におけるVPNトンネルに付加される仮想インタフェイスに対して同一のアドレスを割り当てるとともに、第2の拠点における端末の接続先となる端末に対して前記アドレスとは異なるとともに全ての第2の拠点間で共通なアドレスを割り当て、前記アドレス変換手段はこのアドレスに基づき通信データのアドレスを変換することを特徴とする請求項12記載の複数拠点間の接続装置。

【請求項14】 第1の拠点と複数の第2の拠点とがそれぞれVPNを介して接続されたネットワークにおいて第1の拠点とグローバルネットワークとを接続する接続装置であって、

前記第2の拠点では一の端末のみがVPN接続を行うとともに、この端末が第1の拠点における特定の端末と接

続する場合には、

全ての第2の拠点におけるVPNトンネルに付加される仮想インタフェイスに対して同一のアドレスを割り当てるとともに、第2の拠点における端末の接続先となる端末に対して前記アドレスとは異なるとともに全ての第2の拠点間で共通なアドレスを割り当て、VPNトンネルを通る通信データの送信元アドレス又は送信元アドレスとして前記アドレスを用いることを特徴とする複数拠点間の接続装置。

【請求項15】 前記アドレスに基づきVPNトンネル内を通過する通信データの送信元又は送信先アドレスをVPN接続ごとに変換するアドレス変換手段を有することを特徴とする請求項14記載の複数拠点間の接続装置。

【請求項16】 前記アドレス変換手段による変換されたアドレスに基づき接続先を振り分ける接続先振り分け手段を有することを特徴とする請求項13又は15何れか1項記載の複数拠点間の接続装置。

【請求項17】 第2の拠点を包含する第3の拠点内において未申請のグローバルアドレスが使用されておらず、この第2の拠点では一の端末のみが第1の拠点に対してVPN接続を行う場合において、VPN接続の際に、第2の拠点が新たに意識する第1の拠点内の端末に対して申請済みグローバルアドレスを別名アドレスとして割り当て、前記アドレス変換手段はこのアドレスに基づき通信データのアドレスを変換することを特徴とする請求項12～16何れか1項記載の複数拠点間の接続装置。

【請求項18】 前記アドレス変換の際に用いる全ての別名アドレスを予め備えていることを特徴とする請求項12～17何れか1項記載の複数拠点間の接続装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は複数の拠点のVPN接続を支援するための方法及び装置に関するものである。より詳細には、複数の拠点をVPN接続装置で使用しているアドレスが重複する可能性がある場合に対処するための方法及び装置に関するものである。

【0002】

【従来の技術】近年、グローバルネットワークで分断された複数の拠点を接続する手段としてVPN(Virtual Private Network: 仮想私設網)が利用されている。VPNは、後述するVPNトンネリングなどの技術によって実現される。このVPNを用いた通信では、通信データを必要に応じて暗号化している。これにより盗聴や改竄などの可能性があるインターネット等のネットワークを介する通信を、あたかも専用線接続した場合の通信のように安全性を確保して行うことができる。

【0003】VPNトンネリングとは、中継装置として機能するVPN接続装置が、通信データ全体に新たな送

信先アドレス及び送信元アドレスを付け、これを相手先のVPN接続装置に送信する技術である。このとき元のデータは必要に応じて暗号化される。新たに付けられる接続先アドレス及び接続元アドレスは、各拠点のVPN接続装置のアドレスである。VPN接続装置から送出されたデータは、接続先の拠点にあるVPN接続装置で元の送信元アドレスと送信先アドレスを持つデータに復元される。これにより、各拠点のVPN接続装置さえグローバルアドレスを持っていれば、このVPNトンネリングを利用することができる。

【0004】VPNトンネリングの実装には様々な方法がある。その一つの方法としては、VPNを利用する両拠点のVPN接続装置に同一の仮想的なネットワーク(VPNトンネルと呼ぶ)に接続された仮想インタフェイスを付加し、このVPNトンネルを経由する通信データに対してVPNトンネリングを行うという方法がある。つまり、VPN接続装置に付加された仮想インタフェイスを通してVPNトンネルに入る通信データは、VPN接続装置により必要に応じて暗号化が行われ、VPN接続装置からVPN接続先の拠点内のVPN接続装置宛の通信データとして再構成された後、配送される。ここで再構成されたデータは、仮想インタフェイスではなくVPN接続装置の実インタフェイスを通して相手のVPN接続装置の実インタフェイスに到着する。このデータを受け取ったVPN接続装置は、必要に応じて送信元のVPN接続装置用の暗号鍵を用いて復号化し、元のデータに復元する。ここで、復元されたデータには最初の送信元アドレスと送信先アドレスがついている。このデータは、復元を行ったVPN接続装置の仮想インタフェイスを経由してVPN接続装置に入ってきたデータとして扱われる。

【0005】この方式を使う場合、暗号通信の指定をルーティングの指定として扱うことができるため、アプリケーションにおいて暗号通信のための制御を行わなくて良いことになる。なお、VPNトンネルの片側が直接クライアントマシン(クライアント端末)に接続されている形態のVPNをエンド・トゥ・ステーション型VPNと呼び、通常の方式であるステーション・トゥ・ステーション型VPNと区別する。

【0006】しかしながら、複数の拠点をVPNなどで相互接続すると、各拠点で使用しているプライベートアドレスが重複する場合がある。この場合、そのまま接続することはできない。これをプライベートアドレスの重複問題と呼ぶ。また、この問題は、接続する拠点同士で使用しているプライベートアドレスが重複しなくても、ある拠点がその拠点を包含する上位の拠点を持っている場合には、上位の拠点を含めて使用しているプライベートアドレスが重複しても発生する。例えば、ある拠点Aがそれを包含する上位の拠点Bで使われているプライベートアドレスを接続先として認識している場合、拠点A

が他拠点Cと接続するとき上位の拠点Bで使用されているアドレスを拠点Cが使用していると、拠点A内のマシンはそのアドレスが示すマシンを特定できなくなってしまう。よって、プライベートアドレスの重複問題は、その拠点が接続先として認識している拠点の中で、その拠点を包含する最上位の拠点において発生するか否かで考えなければならない。

【0007】なお、「グローバルアドレス」とは、インターネットなどのグローバルなネットワークにおいて一意に用意されたマシン識別子である。グローバルアドレス利用のためには然るべき権威に対する申請が必要である。現在のインターネットで使用されているグローバルアドレスは、数の不足の問題が深刻化しつつあり、新たにグローバルアドレスを大量に確保することは困難である。この問題はグローバルアドレスの枯渇問題と呼ばれている。

【0008】また、「プライベートアドレス」とは、利用者が任意に割り当てて使うことができるアドレスである。一般的に、プライベートアドレスを送信元アドレスあるいは送信先アドレスに使用している通信データは、インターネットなどのグローバルなネットワークに直接流出することが禁止されている。但し、後述するVPNトンネリング等の技術によって、新たに送信元あるいは送信先アドレスとしてグローバルアドレスを付加することによりプライベートアドレスが隠蔽されるのであれば、このようなデータがグローバルネットワークに流出することは許される。

【0009】また、「拠点」とは、複数の端末が接続されたネットワークあるいはサブネットワーク又は1台の端末のことを指す。LANやイントラネットがその例である。各拠点では、プライベートアドレスに基づくアドレス体系で独自に端末やホストマシンを管理している場合がある。

【0010】従来、前述したようにVPN接続の際などに生じるプライベートアドレスの重複問題に対しては、以下のような方法が採られてきた。

【0011】(A) 外部接続性の放棄

VPN接続をしている間、自拠点内のマシンは接続先拠点内のマシン以外とは接続が行われないようにする。

【0012】(B) アドレス付け替え

少なくとも一つの拠点のアドレスを拠点間で重複しないように付け直す。

【0013】(C) グローバルアドレスの付け替え

前記(B)の場合において、付け直すアドレスとしてグローバルアドレスを使用する。この方法では、一度グローバルアドレスを付けた拠点が、それ以降さらに多重にVPN接続を行う際にはアドレス衝突の問題を起こさない。その点で、この方法は(A)よりも優れているといえる。ここで「ある拠点(以後、拠点Aと呼ぶ)が多重にVPN接続する」とは、拠点Aが複数の拠点B～Zと

同時にVPN接続することを意味する。このとき、拠点Aに対してVPN接続している別拠点B～Z間において、相手拠点到属しているマシン同士の接続が可能である必要はない。

【0014】(D) アドレス変換装置による非共通別名アドレス利用

拠点間の接続境界点にアドレス変換装置を設置し、別名アドレスを利用する。別名アドレスは、お互いの拠点におけるアドレス体系の中で各拠点の管理者が相手の拠点にあるマシンのアドレスに対して用意し、アドレス変換装置に登録しておく。自拠点内では相手のアドレスとして別名アドレスを使用し、通信データが相手の拠点に入る際にアドレス変換装置により、通信データの送信先アドレスとして使用された別名アドレスを実際のアドレスに変換する。このとき同時に、送信元アドレスを送信先の拠点における別名アドレスに付け替える。

【0015】(E) アドレス変換装置による共通別名アドレス利用

接続を行う拠点間で重複しないアドレスを確認して共通の別名として前記(D)と同様に運用する。前記(D)の場合よりも管理が楽になるという利点を有している。

【0016】(F) アドレス変換装置なしの共通別名アドレスの利用

前記(D)の場合で、接続を行う拠点内のマシンそのものが別名アドレスを直接扱うことができるようにする。前記(D)と違い、アドレス変換装置は使用しない。相手の拠点のマシンと接続するときには別名アドレスを使用する。

【0017】(G) 別名アドレスとしてグローバルアドレスの利用

前記(C)(D)(E)の場合で、別名アドレスとして正規に取得したグローバルアドレスを用いる。接続の準備の際に各拠点のアドレスの情報を参照する必要がないという特徴を持つ。

【0018】

【発明が解決しようとする課題】本発明は、以下の課題を全て解決することを目的としている。以下の課題は、従来の方法で部分的に解決されている場合もあるが、全てを同時に解決するような方法は、本発明を除いて存在しない。

【0019】課題1. 接続性確保

VPN接続を行う2つの拠点内のマシンが、VPN接続前に通信可能な全てのマシン(拠点外のマシンを含む)と、VPN接続後も接続可能に維持する手段を提供する。前記(A)の方法はこの条件を満たさない。

【0020】課題2. アドレス付け替えの回避

前記(B)(C)の方法では、アドレスの付け替え作業には一般に大きな手間がかかる。また、既に運用されているネットワークの場合は変更が事実上できない場合が多いため、現実的な方法ではない。そこで、従来使用し

ていたアドレスを使い続けることができる手段を提供する。

【0021】課題3．片側拠点の管理情報の非利用
前記(D)(E)(F)の方法において、プライベートアドレスの範囲内で別名アドレスを用意するという作業は、拠点内の管理方針と矛盾を起ささないようにする必要がある。このため管理者の権限を持つものが判断することが望ましいが、これは一般的に手間がかかるものである。そこで、少なくとも片側の拠点内の管理方針は参照しなくても済む手段を提供する。

【0022】課題4．アドレス交渉の回避
前記(E)(F)の方法では、VPN接続に先立ち、接続する複数の拠点を持つアドレス体系の中で重複しない範囲を特定する必要がある。この特定のためには行う交渉は一般に手間がかかるものである。そこで、このような交渉作業なしで接続を確立する手段を提供する。

【0023】課題5．多重接続時の再設定の回避
前記(B)(E)(F)の方法では、さらに別の拠点を接続する場合、先の2つの拠点では重複しなかったアドレスが新たに重複する場合がある。この場合、新たに重複しないアドレスを用意し接続ホストの別名アドレスを用意し直す必要がある。この作業は一般に手間がかかるものである。そこで、従来のVPN接続環境の再設定をすることなく新たなVPN接続が可能な手段を提供する。

【0024】課題6．アドレス情報の非開示
前記(B)(D)(E)(F)の方法では、VPN接続を行う際に互いの拠点のアドレス情報を提供する必要がある。これはセキュリティ上好ましくないものである。そこで、互いの拠点のアドレス情報を提供することなくVPN接続が可能な手段を提供する。

【0025】課題7．片側拠点の設定の簡易化
前記(B)(D)(E)(F)(G)の方法では、VPN接続を行う拠点の双方において、VPN接続のために必要になるアドレスに関する手続(自拠点内VPN接続装置に追加される仮想インタフェイスへのアドレス付け、相手拠点内マシンの別名アドレスの用意など)が必要である。そこで、VPN接続を行う拠点のうち、片側の拠点がVPN接続のために必要になるアドレスに関する手続を行えばVPN接続が可能な手段を提供する。これは片側をユーザであると考えた場合、ユーザの負担を減らすことを意味する。また、これは前記課題6を包含するものである。

【0026】課題8．グローバルアドレス大量消費の回避

前記(C)(G)の場合、VPNを経由して接続するマシンの数のグローバルアドレスが必要になる。したがって、マシン数が多くなる場合、現在のインターネットのアドレス体系(IPv4)におけるグローバルアドレスの大量取得は困難であるという理由からこの方法の実現は

困難になる。そこで少数のグローバルアドレスの使用でVPN接続が可能な手段を提供する。

【0027】課題9．接続拠点増加時のグローバルアドレス消費量増加の回避

前記課題8において、さらに、拠点Sが複数の拠点に対して多重にVPN接続を行う際に、拠点Sから見た接続先拠点数の増加に対して、使用するグローバルアドレスの数が増加しない手段を提供する。

【0028】

10 【課題を解決するための手段】本発明は、従来の方法(D)の「アドレス変換装置による非共通別名アドレス方式」を基本として採用し、これを拡張したものである。従来の方法(D)を基本として採用することにより、課題1(接続性確保)、課題2(アドレス付け替えの回避)、課題4(アドレス交渉の回避)、課題5(多重接続時の再設定の回避)は達成される。また、方法(D)には、課題8(グローバルアドレス大量消費の回避)、及び課題9(接続拠点増加時のグローバルアドレス消費量増加の回避)は直接関係しないことになるのだが、本方法では後述するようにグローバルアドレスを使用するため、検討を要する。

【0029】本発明が、方法(D)を元にしていても拘わらず、本願で他の方法の問題点を上げている理由は、方法(D)の拡張を行うにあたって、他の方法の問題点を持ち込まないことを明記するためである。

【0030】また、本発明で採用するVPNの方式は、第2の拠点と第1の拠点とをエンド・トゥ・ステーション型で接続する。したがって、すなわち第2の拠点であるクライアント拠点側のマシン(端末)のうち、VPNトンネルを経由して接続を行うものは、VPNトンネルごとに1台のみである。そのマシンは、VPNトンネルの仮想インタフェイスが付加されたクライアントマシンそのものである。通信データの送信元として使用されるアドレスは、データが出力されるインタフェイスのアドレスであるため、VPNトンネルの内部を通過する通信データのうち、クライアント側のマシンを表すものとして使われるアドレスは、仮想インタフェイスのアドレスだけになる。また、また、第1の拠点であるサーバ側拠点は、複数のマシンが接続されたLANである。

【0031】本発明では、前記(D)の方法に加えてさらに2つの工夫を行う。この2つの工夫が、本発明の本質である。以下、その内容を説明する。

【0032】第1の工夫は、VPN接続時にクライアントが新たに認識するアドレスとしてグローバルアドレスを使うという方法である。VPN接続を行うと、VPN接続を行うマシンは、接続前から使用しているアドレスに加えて、新たなアドレスを認識することになる。それは、VPNトンネルの両端となる仮想インタフェイスのアドレス2つと、クライアントが接続を行う第1の拠点であるサーバ拠点内のマシンのアドレスである。前記

(D) の方式を使うと、クライアント側で新たに認識するアドレスとサーバ拠点側で意識するアドレスは異なることになる。そのうちのクライアント側で認識するアドレスだけでグローバルアドレスを使用し、サーバ側では、前記(D) の方法と同じくサーバ拠点側のプライベートアドレスを割り振る。ここで使用されるグローバルアドレスは、グローバルネットワーク内でのルーティングで使用されるものではなく、あくまで、VPNの内側のみで使用されるアドレスである。

【 0033 】この第1の工夫により、前記課題3、6及び7が解決する。その理由を以下に説明する。

【 0034 】まず、課題3(片側拠点の管理情報の非利用)が解決される理由を説明する。この工夫では、第2の拠点であるクライアント拠点が新たに認識するアドレスとしては、グローバルアドレスだけになるようにする。グローバルアドレスはクライアント側の拠点内で使用されるプライベートアドレスと重複することはない。よってクライアント拠点にいるユーザがアドレス変換装置の動作設定の際に、クライアント側で使っていないプライベートアドレスの情報を入力することや、クライアント拠点内のマシンのうち、VPNを経由して通信を行うマシンのアドレス(プライベートアドレス)を入力する必要はない。これにより課題3が解決される。

【 0035 】次に、課題6(アドレス情報の非開示)が解決される理由について説明する。開示すべきではないアドレス情報とは、各拠点内で使用されているプライベートアドレスの情報である。本方法を使った場合、第2の拠点であるクライアント拠点で必要な設定は、クライアントのVPN接続装置と第1の拠点であるサーバ拠点のVPN接続装置のVPN接続を確立するためのものだけでよい。このときにクライアント側として使用されるアドレスは、クライアント拠点側のファイアウォールで使用されるアドレスであり、サーバ拠点でもファイアウォール上にあるVPNサーバのアドレスである。このアドレスは、VPNトンネリングによってカプセル化された後に付加されるアドレスとして使われる。設定の際に、クライアント拠点内のプライベートアドレスの情報を求められることはないので、この情報の流出は避けられる。ここで、サーバ拠点からクライアントマシンへのVPNトンネル内を経たアクセスは、クライアントマシンのプライベートアドレスではなく、クライアント側の仮想インタフェースのアドレスが使用される。また、サーバ拠点では、クライアントのアドレスとしてグローバルアドレスを意識するのではなく、各クライアントにサーバ拠点で使用しているプライベートアドレスを割り当てることになる。しかし、この割り当ては、サーバ拠点側に設置された装置への設定だけで済む。よってその情報はクライアント拠点に知らされないため、アドレス情報は流出しない。

【 0036 】課題7(片側拠点の設定の簡易化)を達成

するために、本方法では、クライアントが認識するアドレスとしてのグローバルアドレスをサーバ拠点側で予め用意する。そして、エンド・トゥ・ステーション型VPNの特徴として、第2の拠点であるクライアント側の仮想インタフェースのアドレス割り当てを、第1の拠点であるサーバ拠点側から行うことができるため、これを利用する。

【 0037 】第2の工夫は、複数のマシンを示すものとして同一のグローバルアドレスを利用することである。つまり、複数のクライアント拠点が認識するアドレスとして、そのアドレスが互いに別のマシンを示すものであっても、同じアドレスの組を使用するのである。

【 0038 】この第2の工夫により、課題8(グローバルアドレス大量消費の回避)及び課題9(接続拠点増加時のグローバルアドレス消費量増加の回避)が解決される。

【 0039 】

【 発明の実施の形態 】(第1の実施の形態)以下に、本発明の第1の実施の形態にかかる複数拠点間の通信について図1を参照して説明する。図1はネットワーク構成図である。なお、図において、実アドレスについては「<>」を付すとともに、別名アドレスについては「()」を付すことにより両者を区別している。また、図において、実線矢印は接続要求が存在する組を表し、点線はVPNトンネルを表している。

【 0040 】図1に示すように、第1の拠点100と第2の拠点200-1~200-nは、例えばインターネット等のグローバルアドレスに基づくネットワーク1を介して接続されている。そこで本実施の形態では、このネットワーク1を利用して第1の拠点100と複数の第2の拠点200-1~200-nの間にそれぞれVPNを構築し、第1の拠点100と第2の拠点200-1~200-n間で通信を行うものである。なお、第2の拠点200-1~200-nは、それぞれ第3の拠点300-1~300-nに包含されている。例えば、第3の拠点と第2の拠点との関係が一のネットワークとそのサブネットワークという関係になっている場合である。

【 0041 】ここで、VPN接続は、前述したエンド・トゥ・ステーション型である。すなわち、第2の拠点200-1~200-n内のクライアントマシン201(クライアント端末)はそれぞれ1台のみ設置されている(図1の201-1~201-n)。また、各拠点200-1~200-nのクライアントマシン201-1~201-nはそれぞれVPN接続機能部202-1~202-nが実装されている。各クライアントマシン201-1~201-nは、独自のプライベートアドレスPAC1~PACnを有している。また、各クライアントマシン201-1~201-nは、前記プライベートアドレスの他にグローバルアドレスGAC1~GACnを有している。第2の拠点200のそれぞれには、クラ

11

クライアントマシン201のプライベートアドレスをグローバルアドレスに変換するためにPROXYサーバやファイアウォールなどのアドレス変換部(図示省略)を有している。これにより、第2の拠点200はネットワーク1と直接通信し、VPNを構築可能としている。なお、各クライアントのプライベートアドレスは、複数の第2の拠点200間で重複していてもよい。

【0042】第1の拠点100には、主装置110内に1つのVPN接続機能部111が設けられている。このVPN接続機能部111は独自のプライベートアドレスPAS0を有する。また、このVPN接続機能部111はこのプライベートアドレスPAS0の他にグローバルアドレスGAS0を有している。これによりネットワーク1と直接通信し、VPNを構築可能としている。また、この主装置110にはアドレス変換機能部112が設けられている。

【0043】また、第1の拠点100には、主装置110に複数のマシン101-1~101-nがLANを介して接続している。各マシン101-1~101-nは、それぞれプライベートアドレスPAS11~PAS1nを有している。これらのプライベートアドレスPAS11~PAS1nは、第2の拠点200の各クライアントマシン201-1~201-nのプライベートアドレスPAC1~PACnと重複していてもよい。

【0044】以下、第1の拠点100と第2の拠点200間における通信の基本手順について説明する。なお、以下において、アドレスを表す記号としてPAで始まるものはプライベートアドレスを表すものとし、GAで始まるものはグローバルアドレスを表すものとする。

【0045】(1) VPN接続準備

まず、VPN接続の準備として、第2の拠点200-1~200-nのVPN接続機能部202-1~202-nを、第1の拠点100の接続機能部111が接続要求を受ける対象として予め登録しておく。以下、第1の拠点100内のマシン101-1と第2の拠点200-1内のマシン201-1間の通信を例にとって説明する。

【0046】第1の拠点100は、VPN接続後のクライアントマシン201-1の仮想インタフェースに割り振る別名アドレスPAS31と、第1の拠点100のVPN接続機能部111に付加される仮想インタフェースの実アドレスPAS21を用意する。これはどちらも第1の拠点100内のプライベートアドレスである。

【0047】ここで、アドレスの割り振りには登録時に静的に割り振る方法と、VPN接続確立時に動的に割り振る方法の2つがあり、本発明ではどちらであるかは限定しない。ここでは前者の静的に割り振るものとする。また、この時、必要であれば暗号鍵の準備を行う。片側で用意した暗号鍵で暗号化されたデータが、もう片側で用意した暗号鍵で復号化することが可能であるようにしておく。本方法では、この暗号鍵が共通なものであるか

12

非共通なものであるかは限定しない。

【0048】また、本発明では各クライアントマシン201-1~201-nごとに第1の拠点100内のマシン101-1~101-nの別名アドレス用のグローバルアドレスを実際の第1の拠点100内のマシン101-1~101-nに対応づける必要がある。ここではクライアントマシン201-1がマシン101-1に接続要求を持っていることになっているので、グローバルアドレスGA1を、マシン101-1の実アドレスPAS11に対応づけるように設定する。この設定はアドレス変換機能部112の動作に反映される。

【0049】さらに、後述するアドレスの割り当て時に用いるグローバルアドレスGA2及びGA3を予め用意しておく。前記グローバルアドレスGA1、グローバルアドレスGA2及びGA3は、第1の拠点100で使用するものとして所定の権威(例えばグローバルネットワークがインターネットならばNIC)に申請済みの範囲内のもを使用するのが好ましい。これにより、第2の拠点200において、クライアントマシン201が第1の拠点100以外に接続する際に、当該他の接続先とグローバルアドレスの重複を起こすことがない。

【0050】(2) 接続要求の発行

以降は第2の拠点200-1内のクライアントマシン201-1から第1の拠点100内のマシン101-1へ接続を行う際の処理の流れについて説明する。まず、クライアントマシン201-1のVPN接続機能部202-1が、第1の拠点100のVPN接続機能部111に接続要求を発行する。

【0051】(3) クライアントの認証

VPN接続機能部111はクライアントマシン201-1が登録されたクライアントマシンであることを確認するための認証を行う。

【0052】(4) VPN接続の確立

VPN接続機能部202-1及びVPN接続機能部111はクライアントマシン201-1と第1の拠点100との間のVPN接続を確立する。これは仮想インタフェース及びVPNトンネルを利用可能な状態にすることを指す。

【0053】この時に必要なアドレスは、第1の拠点100側のVPN接続機能部111に予め登録してあるものを使用する。このアドレスは、第1の拠点100側のVPN接続機能部111に付加される仮想インタフェース用の実アドレスとしてPAS21、その別名アドレスとしてGA2、クライアントマシン201-1側のVPN接続機能部202-1に付加される仮想インタフェース用の実アドレスとしてGA3、その別名アドレスとしてPAS31の計4つになる。このように本方法では、クライアントに付加される仮想インタフェースの実アドレスは第1の拠点100ごとに共通のグローバルアドレスGA3を使用し、第1の拠点100のVPN接続機能

部111の仮想インタフェイスに付加されるアドレスとしては、予め前記(1)において登録してあるものを使用する。

【0054】以上で、第1の拠点100と第2の拠点200-1間でVPNが構築された。以降は、クライアントマシン201-1がVPNトンネルを介して第1の拠点100内のマシンと通信を行う過程について説明する。

【0055】(5)クライアントマシンから第1の拠点100内マシンへの通信データの送信

クライアントマシン201-1から第1の拠点100内のマシン101-1への通信を行う。この時、通信データはVPNトンネルを経由して第1の拠点100内のマシンへ向かう。クライアントマシン201-1で生成され、はじめにVPNトンネルに出されるデータには仮想インタフェイスのアドレスGA3が送信元アドレスとして付加される。このアドレスは上で示したように、第1の拠点100にとってはクライアントマシンによらず固定のグローバルアドレスである。このデータの送信先アドレスにはマシン101-1の別名アドレスであるグローバルアドレスGA1が使用される。ここで、このアドレスは、前記(1)でマシン101-1に対応づけられたグローバルアドレスである。

【0056】(6)接続先の振り分け

第1の拠点100にある主装置110内のアドレス変換機能部112では、VPNトンネルを経由して仮想インタフェイスから入ってきた通信データの送信先アドレス及び送信元アドレスを、第1の拠点100内で使用されるプライベートアドレスに変換する。アドレス変換機能部112は、各クライアントマシンが接続するマシンのアドレスを管理しており、適切な送信先にアドレスを付け替えることによって接続先を振り分ける。この時、各クライアントマシンごとに個別のVPNトンネルを使用することになっているので、データが経路する仮想インタフェイスによってどのクライアントから来たデータであるかを認識する。クライアントマシン201-1からの通信データの場合、送信先アドレスGA1をPAS11に変換する。クライアントマシンが接続するマシンの数が第1の拠点100内に複数ある場合は、変換前の送信先アドレスにしたがい接続先を特定する。また、送信元アドレスは前記(1)でクライアントの登録の際に用意した、第1の拠点100内で使用するクライアントの別名アドレスに変更する。クライアントマシン201-1からの通信データの場合、送信元アドレスはGA3からPAS31に変換される。

【0057】(7)クライアントマシンに向けての通信
第1の拠点100内のマシンから、第2の拠点のクライアントマシンに向けての通信に対しては、前記(6)で示しアドレス変換の逆を行うようにする。この時、クライアントマシンにつけられた第1の拠点100内のアド

レスを送信先アドレスとして持つ通信データが、そのクライアントマシンに接続されたVPNトンネルを経由するようになっていなければならない。これは、第1の拠点100内のデータ配送制御機構により実現すればよい。

【0058】(第2の実施の形態)次いで、本発明の第2の実施の形態にかかる複数拠点間の通信について図2及び図3を参照して説明する。図2はネットワークの接続要求を説明する概念図、図3はネットワーク構成図である。なお、第1の実施の形態と同一の要素については同一の符号を付した。

【0059】本実施の形態では、図2に示すように、第2の拠点200-0内の複数のクライアントマシン201-01~201-0mがVPNを経由して第1の拠点100内のマシン101-1に接続したいという要求がある場合について説明する。

【0060】このような接続形態についても、以下に示す手順により、図3のようにネットワーク構成を変更すれば、クライアントマシン側の拠点中のマシンの数を一つに抑え前記図1の基本構成に当てはめることができる。これにより前記課題8を解決する。

(1)クライアントマシン201-01~201-0mの全てにVPN接続機能部装置202-01~202-0mを内蔵させる。

(2)クライアントマシン201-01~201-0mの各マシンに対し、それぞれ1台のみを構成要素とする部分拠点210-01~210-0mがあると考える。

(3)部分拠点210-01~210-0mから第1の拠点100に対して個別のVPNを構築する。

【0061】(第3の実施の形態)次いで、本発明の第3の実施の形態にかかる複数拠点間の通信について図4を参照して説明する。図4はネットワーク構成図である。なお、第1及び第2の実施の形態と同一の要素については同一の符号を付した。

【0062】本実施の形態では、第2の実施の形態と同様に、第2の拠点200-0内の複数のクライアントマシン201-01~201-0mがVPNを経由して第1の拠点100内のマシン101-1に接続したいという要求がある場合について説明する。

【0063】図4に示すように、第2の拠点200-0にVPN接続装置202-0を設置し、VPN接続装置202-0と第1の拠点100の主装置110の間でVPN接続を行う。ここで、VPN接続装置202-0はクライアントマシン201-01~201-0mからの通信データの送信元アドレスを自分のアドレスに置き換える機能を持つ変換部220を内蔵するものとする。インターネットの世界においてこの技術は「IPマスカレード」又は「NAPT」等と呼ばれる。これにより第1の拠点100から見た場合、クライアントマシン201-01~201-0mからの全ての通信は、VPN接続

装置202-0からの通信であるように見える。クライアントマシン201-01~201-0mにはそれぞれ、第3の拠点300-0のプライベートアドレスPAC01~PAC0mがついているとすると、最初にこのアドレスを送信元アドレスとしている通信データが、VPN接続装置202-0を通過する際、送信元アドレスとして、VPN接続装置202-0のアドレスGA3に置き換わる。さらに、このアドレスは図1に示したものと同じく、主装置110のアドレス変換機能部112を通過する際に、別名アドレスPAS30に置き換わる。このPAS30は第1の拠点100のプライベートアドレスである。このように、VPN接続装置202-0だけからなる拠点200-00を第2の拠点として考えることによって図1の構成に置き換えることができる。この方法で課題8を解決することができる。同様の方法は、クライアント側である第2の拠点に限らず、サーバ側の第1の拠点においても使うことができるが、ここでは省略する。

【0064】(第4の実施の形態) 次いで、本発明の第4の実施の形態にかかる複数拠点間の通信について図5を参照して説明する。図5はネットワーク構成図である。なお、前述した各実施の形態と同一の要素については同一の符号を付した。

【0065】本実施の形態では、第2の拠点200-1が第1の拠点100内の複数のマシン201-1及び201-2に接続を行う場合を示す。この場合にはVPNトンネルを経由して接続するマシンの数だけグローバルアドレス(GA11, GA12の2つ)が必要になる。第1の拠点100内のマシンの別名アドレスとして使用されるグローバルアドレスの総数は、第1の拠点100に接続する第2の拠点200-1~200-nの中で、同時に接続を行う第1の拠点100内のマシンの総数の最大値になる。ここで、この数はクライアント側拠点である第1の拠点200の数そのものには影響を受けない。したがって、依然として課題9は解決されている。すなわち、例えば図5に示すように、第2の拠点200-2が第1の拠点100内のマシン100-2と接続する場合には、このマシン100-2に割り当てる別名アドレスとして、グローバルアドレスGA11を用いることができる。つまり、第2の拠点200-1と第1の拠点100の接続用に用いた別名アドレスと同一のアドレスを、第2の拠点200-2と第1の拠点100の接続時にも用いることができる。

【0066】(第5の実施の形態) 次いで、本発明の第5の実施の形態にかかる複数拠点間の通信について図6を参照して説明する。図6はネットワーク構成図である。なお、前述した各実施の形態と同一の要素については同一の符号を付した。

【0067】本実施の形態では、第1の拠点100に接続する第2の拠点200-1と第2の拠点200-2が

相互に通信を行う場合を示す。この場合には、第2の拠点200-1から見ると第2の拠点200-2内のクライアントマシン201-2は第1の拠点100に存在しているように見える。逆に第2の拠点200-2から見た場合、第2の拠点200-1内のクライアントマシン201-1が第1の拠点100に存在しているように見える。この場合、お互いに相手のアドレスとして同じアドレスGA1を意識することになる。

【0068】また、異なるVPN方式に対応した主装置100を複数用意することにより、異機種間VPN通信が可能になる。

【0069】

【発明の効果】現在のインターネットのアドレス体系(IPv4)においてグローバルアドレス不足の問題は深刻なものと考えられている。十分なグローバルアドレスを持つ新たなアドレス体系(IPv6)への以降の検討が進められているが、この新たなアドレス体系が主流に使われるようになるまでには、まだ時間がかかると考えられている。しかも、現在使用されているアドレス体系がインターネット上で使われなくなることはなく、将来的にも共存環境が続くと言われている。

【0070】一方、アドレスが大量に利用できるという環境にあれば、コンピュータネットワークの使用方法も変わってくると考えられる。例えば一台のホストマシンを仮想的に複数台に見せる技術などにより、小規模な環境を大量に扱うことなどが可能になる。この場合アドレスも大量に消費することになる。また、1台のマシンが複数のネットワークに仮想的に接続されるという形でエクストラネットを構築するということも考えられる。本発明は、このような形態のエクストラネット構築を考慮に入れている。この場合、1台のマシンで複数のアドレスを使用することになり、ネットワーク全体としてはやはりアドレスが大量に必要な。このようにこれらの実現の際にはグローバルアドレスの枯渇問題が大きな障害になっているのである。

【0071】グローバルアドレス枯渇問題の対策としてプライベートアドレスが各拠点内で広く使われつつある。しかし近年のエクストラネットの発展に伴い、複数の拠点をVPN接続する状況が増えてきており、この際に発生するプライベートアドレスの重複問題が深刻化することになった。従来、この問題を解決するためには多大な設定の手間がかかっていた。

【0072】前述したように、本発明では、VPN接続の関係に関して接続拠点の役割をサーバ側である第1の拠点とクライアント側である第2の拠点に分け、第1の拠点到本発明の装置を設置することによって、プライベートアドレスの重複を起こす可能性のあるVPN接続の際に、第2の拠点側の設定負担を軽減することを可能にする。

【0073】これは、グローバルアドレスを別名アドレ

スとして利用することにより、アドレス重複を回避するという手法と、限られた少数のグローバルアドレスを無制限に多数のクライアント拠点との接続のために使うという手法により実現される。

【0074】また、サーバ側である第1の拠点でプライベートアドレスを使う代わりにIPv6のアドレス体系の下でアドレス付けを行うことにより、現在のアドレス体系と新たなアドレス体系の共存関係を実現できる。よって実施例に示したサーバレンタルサービスにおいてIPv4とIPv6の共存環境をこの方法により構築することができ、このようなサービス対象者として現在のアドレス体系の拠点をサポートする限り本発明は有用であるといえる。

【0075】本発明には以下のような利用例が考えられる。

【0076】例1．サーバレンタルサービス

各種サーバや電子掲示板やファイル共有環境などをネットワーク上で提供する。通信経路の安全性はVPNによって確保する。複数の企業に属するマシンをクライアントとして接続し、エクストラネットを簡単に実現することができる。

【0077】利点としては、レンタルという形態をとることで、初期投資のコストが少なく済むということ、必要になったときにすぐに利用できること、短期間での運用が可能であること、サーバの管理をサービスの提供者に委託可能であることなどがある。また、企業のファイアウォールの設定は内側から外側への接続は許可される場合が多いので、エクストラネット環境の構築をより簡単に行うための手段になりうる。

【0078】このサービスとを大規模に行う際に、グローバルアドレスの枯渇問題及びプライベートアドレスの重複問題を解決することが必要になってくる。本発明を利用すれば、クライアント側の設定の負担が少ない形でこの問題を解決できる。

【0079】例2．企業内サーバ集中管理センタ

本方式を利用して、企業内でアプリケーションの集中管理センタを構築する。集中管理センタを構築する利点は、企業内で分散していたアプリケーション環境を集中管理することによりTCO（Total Cost of Ownership: 所有に由来する総コスト）を削減することなどがある。例えばソフトウェアのアップグレードに要するコストを抑えることや、重要な情報を守るための機器設置環境を充実させるためのコストを抑えること、システムの管理技術を持つ人材を集中することによって人的コストを削減することなどがある。

【0080】企業内でも他部署に流出を避けたい情報を扱う場合も考えられるので部署単位で暗号通信を使ったVPNを利用することはあり得るためVPNの利用は有用である。また、部署間にまたがったグループを構成する際のネットワーク環境を提供するためにも、ここに示

す集中管理センタは有用である。

【0081】本発明を利用することによって、各部署間でプライベートアドレスが重複するような使い方をしている場合でも集中管理が可能になる。

【0082】例3．アプリケーションサーバレンタルサービス

従来のアプリケーションの流通形態は、アプリケーションをパッケージとして販売し顧客が自分のマシンにインストールして使うという形をとっていた。本発明を利用し、ネットワークを経由してサービスセンタ内のサーバ機に顧客がアクセスすることによって利用できるようにすることを考える。このサービスの利点としては、使用度数に応じた従量課金など料金徴収の方法に多様性を持たせることができることや、クライアント側の設備変更が最小限で済むことなどがある。本発明は安全な通信の確保のためにVPNを利用しているため使用プロトコルの制限が少ないという特徴がある。なお、このサービスも例1と同様の問題を持っており、本発明によってこれらが解決される。

【0083】例4．VPN接続中継システム

VPN接続の要求がある複数の拠点が、中継システムを介して接続を行うことを考える。本発明におけるサーバ側拠点である第1の拠点は、ここで言う中継システムとして機能し、クライアント側拠点である第2の拠点のVPN接続の中継を行う。中継センタが有用になる場合としては、プライベートアドレスの重複問題を解決する手段としてこの中継システムを使う場合や、ファイアウォール越え問題などにより、接続拠点のうち一つもVPN接続の待ち受けができない場合や、各拠点のネットワーク情報を開示せずに接続を行う場合などがある。

【0084】但し、本方法は第2の拠点に1台のクライアントマシンしかないことを前提とするので、接続先としてクライアントマシン1台ではなくそのクライアントマシンの属する上位拠点のマシンへのアクセスを考えると、図4のように、他のマシンをあたかもそのクライアントであるかのように見せるIPマスカレード機能などが必要になる。

【0085】例5．異種暗号方式中継システム

前記例4で示した実施例において、サーバ側拠点である第1の拠点に異なるVPN方式をもとにした複数の主装置を設置することにより、異なる方式のVPN接続装置を持つ拠点を接続するための中継システムとなることができる。

【図面の簡単な説明】

【図1】ネットワーク構成図

【図2】ネットワークの接続要求を説明する概念図

【図3】ネットワーク構成図

【図4】ネットワーク構成図

【図5】ネットワーク構成図

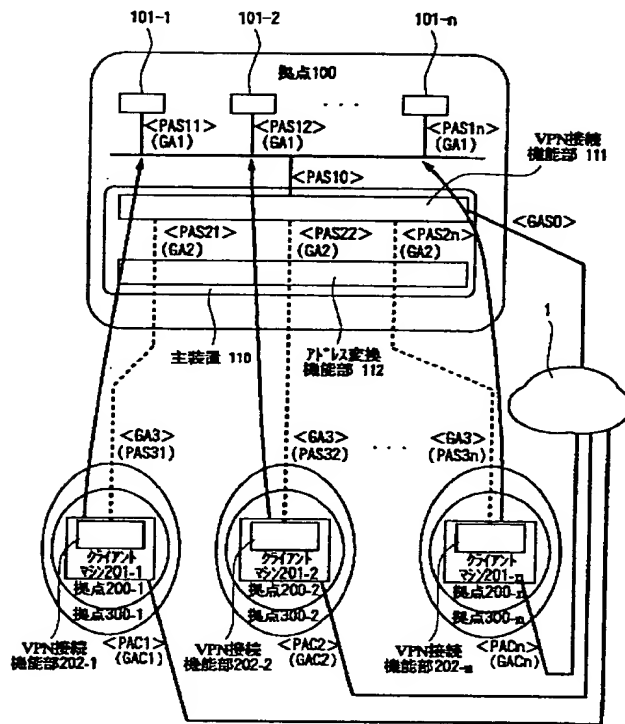
【図6】ネットワーク構成図

【 符号の説明】

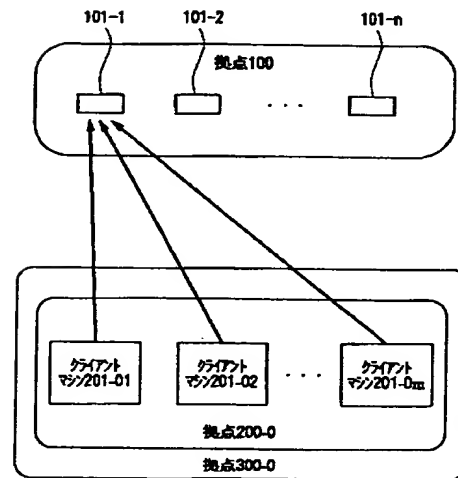
1…ネットワーク、100…第1の拠点、101…マシン、110…主装置、111…VPN接続機能部、112…アドレス変換機能部

2…アドレス変換機能部、200…第2の拠点、201…クライアントマシン、202…VPN接続機能部

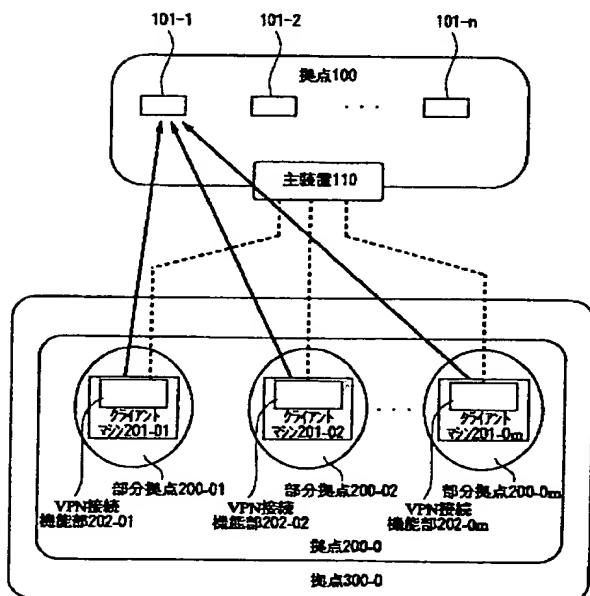
【 図1 】



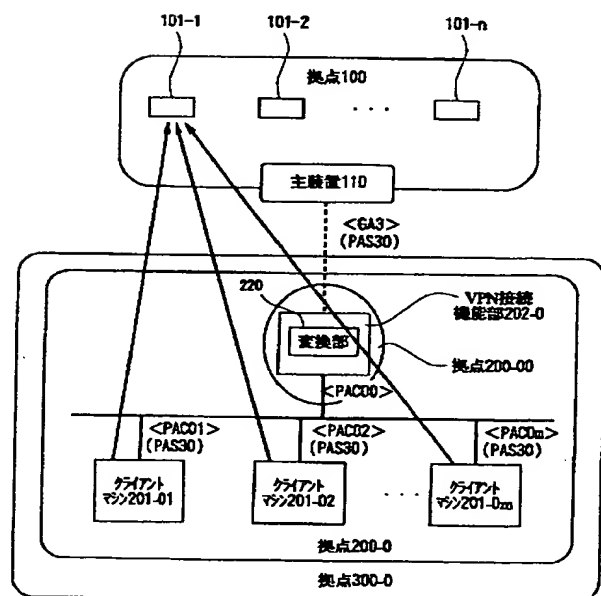
【 図2 】



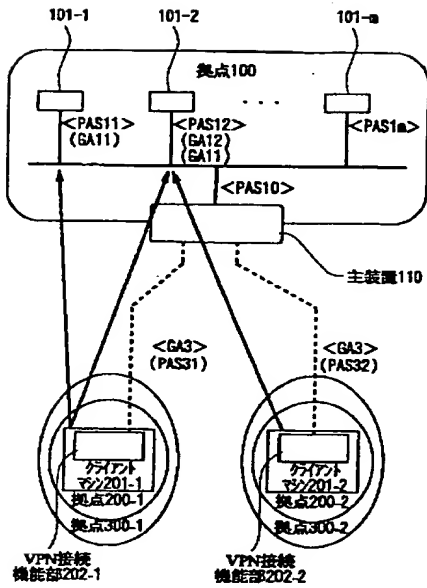
【 図3 】



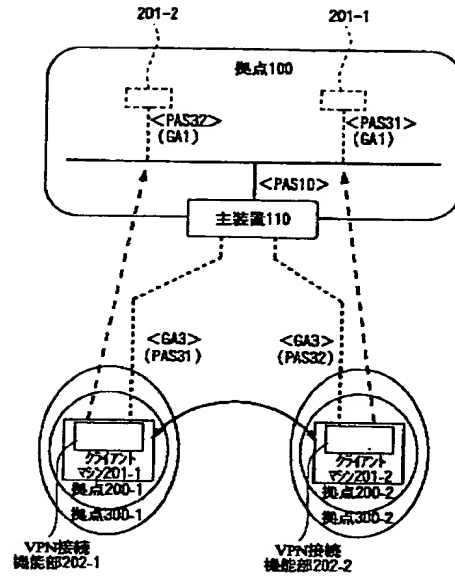
【 図4 】



【 図5 】



【 図6 】



フロント ページの続き

F ターム (参考) 5K030 GA15 GA19 HC01 HD09 LB05
LD16 LD17
5K033 AA04 AA08 AA09 CB09 DA06
EC03
9A001 EB02 EB03 EB04 CC03 CC07
CC08 DD12 EE02 EE03 JJ18
JJ27 KK56 LL03